In the Claims

Please amend Claim 1 and add Claims 21 & 22.

1. (Currently amended) A method of authenticating a transaction, the method comprising:

causing a separate unit to communicate with a device ,

the separate unit being secured and independently

operating from the device, the separate unit configurable to include a first biometric sensor to obtain first biometric characteristics of a user, the first biometric characteristics physically representing the user;

initiating a transaction request using the device;

encrypting the request;

communicating the ~~transaction~~ encrypted request to a third party through the device; and

receiving a signal at the separate unit via the device to authenticate the transaction, wherein the separate unit is caused to request personalized data from the user associated with the device, the separate unit is not to encrypt the transaction but to authenticate the transaction between the device and the third party only when the biometric characteristics of the user is verified, the transaction can only be authenticated when the personalized data is authenticated in the separate unit.

2. (Previously amended) The method of claim 1, wherein the separate unit is further configurable to include a second biometric sensor to acquire second biometric characteristics of the user to ensure that the user is indeed authenticated.

3. (Previously amended) The method of claim 1, wherein the first biometric sensor is a fingerprint sensor to acquire a fingerprint of the user, and the second biometric sensor is a microphone to acquire a voice of the user.

4. *(Original)* The method of claim 1, wherein the device is a personal digital assistant (PDA).

5. *(Original)* The method of claim 1, wherein the device is a telephone.

6. *(Original)* The method of claim 5, wherein the telephone is a cellular telephone.

7. *(Original)* The method of claim 1, wherein the signal used to authenticate the transaction is a high-contrast optical signal.

8. *(Previously amended)* The method of claim 1, wherein said communicating the transaction request to the third party involves a use of a dual-tone audio signal.

9. *(Original)* The method of claim 8, wherein the signal is a dual-tone, multi format (DTMF) signal.

10. *(Original)* The method of claim 8, wherein the signal is an audio frequency shift keying (AFSK) signal.

11. *(Previously amended)* The method of claim 8, wherein the signal is a private line (PL) signal or a wireless signal.

12. *(Previously amended)* The method of claim 1, wherein said initiating a transaction request includes an entry of a personal identification number (PIN) through the keyboard of the device.

13. *(Previously amended)* The method of claim 12, wherein the separate unit is terminated if a PIN entry is attempted more than a predetermined number of times.

14. *(Previously amended)* The method of claim 1, wherein the separate unit further includes a biometric input; and said initiating a transaction request includes receiving biometric data through the biometric input.

15. *(Original)* The method of claim 14, wherein the biometric input is a fingerprint.

16. *(Previously amended)* The method of claim 1, wherein one or both of the transaction request and the authentication signal are encrypted.

17. (Original) The method of claim 16, wherein the encryption is based on public key cryptography.

18. *(Previously amended)* The method of claim 1, wherein the separate unit or device includes a memory; the transaction request and authentication signal constitute a session; and information regarding the session is stored in the memory.

19. *(Previously added)* The method of claim 1, wherein the separate unit is a headset.

20. *(Previously added)* The method of claim 19, wherein the headset includes capability of reading in confidential information from a user associated with the device.

21. *(Inserted)* The method of claim 1, wherein the said encrypting is performed using a one-way encryption algorithm that employs one or many of biometric input, atomic clock and unique session keys.

22. *(Inserted)* The method of claim 1, wherein the said authenticating is performed using a challenge response protocol.